REMARKS

Claims 11 and 13-22 are pending. The Examiner's reconsideration of the rejection in view of the amendments and remarks is respectfully requested.

Claims 11 and 22 have been objected to for an informality. The phrase "and performed inline decryption of the copy of said authorized code is said protected memory" has been amended to "and performed inline decryption of the copy of said authorized code in said protected memory" to correct a spelling error. Entry of the amendment is respectfully requested.

Claims 1, 11 and 22 have been rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner suggested essentially that the lack of an "else" statement renders the claims indefinite.

Applicants respectfully disagree. The claims recite complete and clear method steps which produce a useful and tangible result. Whether an "else" condition exists is not relevant to the claims, which are clearly directed to conditions where "if said original digital signature is verified." Indeed, the claim may be more clearly understood as, for example, an if/then statement. Such a mathematical examination of the claims does not affect the clarity of what is claimed therein. Clearly, one of ordinary skill in the art would understand what is meant by "if said original digital signature is verified." Following the claim language, the claimed limitations are believed to be definite. Accordingly, Claims 11 and 22 are believed to satisfy the

requirements of 35 USC 112, second paragraph. Claim 1 has been cancelled. Reconsideration of the rejection is respectfully requested.

Claims 1-6, 9-16, 18 and 19-22 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al. (USPN 6,397,331) in view of Morgan et al. (USPN 6,185,685). The Examiner stated essentially that the combined teachings of Ober and Morgan teach or suggest all of the limitations of Claims 1, 3-11 and 13-22.

Claims 11 and 22 are the independent claims.

Claims 11 and 22 claim, *inter alia*, "applying an original digital signature to all authorized code; storing said signed authorized code in a protected memory, wherein said protected memory is cryptographically protected; preparing to execute code from the protected memory by verifying a digital signature used to sign said code in accordance with a public key, which corresponds to said original digital signature; and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory."

Ober teaches a method of expanding a secure kernel memory area to accommodate additional software code (see Abstract). Ober does not teach or suggest "branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory" as claimed in Claims 11 and 22. Ober teaches that a secure kernel memory area may be expanded into an unprotected memory area (see col. 2, lines 28-34). Further, Ober teaches that the expansion may be in the form of a cryptographic algorithm or other kernel extension (see col. 2, lines 55-67). Such an

expansion of secure kernel memory does not teach that the protected memory is cryptographically protected – Ober teaches merely that the data in memory is signed. Signed data in a secure kernel memory is not analogous to branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory as claimed in Claims 11 and 22. Indeed, nowhere does Ober teach or suggest cryptographically stored data – for example, the cryptographic algorithm stored in the newly acquired memory is not itself cryptographically protected. The data stored in the newly acquired memory of Ober is merely signed. With regards to the Examiner's suggestion on page 3 of the Final Office Action that digital signing is a type of cryptographic protection, Applicants believe that digital signing is a type of cryptographic protection only to the extent of the creation of the signature itself, as no data is encrypted as the result of a digital signature - digital signatures are cryptographic creations used to verify authenticity of data, not to encrypt data. Therefore, Ober fails to teach or suggest "branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory" as claimed in Claims 11 and 22.

Morgan teaches a system of servers and clients implementing a multi-stage login (see Abstract). Morgan does not teach "branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory" as claimed in Claims 11 and 22. Morgan teaches that the client combines a first split symmetric persistent storage key with a one-way hash value to obtain a persistent storage key for use by the client computer to communicate encrypted data and/or operating programs to and from the persistent storage (see Abstract and col. 4, lines 33-42). Morgan does not teach that the encryption or decryption is performed as a result of branching

(e.g., for inline decryption), essentially as claimed. More particularly, Morgan does not explicitly teach that a processor branches to a copy of the authorized code nor that a processor performs inline decryption of authorized code in a protected memory, essentially as claimed in Claims 11 and 22. Therefore, Morgan fails to cure the deficiencies of Ober.

The combined teachings of Ober and Morgan teach a combined multi-stage login procedure using asymmetric and symmetric keys. The combined teachings of Ober and Morgan do not teach "branching to a copy of said authorized code in said protected memory to begin execution and performing inline decryption of the copy of said authorized code in said protected memory" as claimed in Claims 11 and 22.

Claims 13-21 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. Claims 1 and 3-10 have been cancelled. The Examiner's reconsideration of the rejection is respectfully requested.

Applicants have cancelled Claims 1 and 3-10 from further consideration in this application. Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the present claim cancellations are only for facilitating expeditious prosecution of the allowable subject matter noted by the Examiner. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

For the forgoing reasons, the application, including Claims 11 and 13-22, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: June 25, 2007

/Nathaniel T. Wallace/
Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889